ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra 309 (2007) 497–517

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Homomorphisms, localizations and a new algorithm to construct invariant rings of finite groups

Peter Fleischmann [a,*], Gregor Kemper [b], Chris Woodcock [a]

[a] *Institute of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, CT2 United Kingdom*

[b] *Technische Universität München, Zentrum Mathematik – M11, Boltzmannstr. 3, 85 748 Garching, Germany*

Received 21 April 2005

Available online 20 November 2006

Communicated by Harm Derksen

Abstract

Let G be a finite group acting on a polynomial ring A over the field K and let A^G denote the corresponding ring of invariants. Let B be the subalgebra of A^G generated by all homogeneous elements of degree less than or equal to the group order $|G|$. Then in general B is not equal to A^G if the characteristic of K divides $|G|$. However we prove that the field of fractions $\mathrm{Quot}(B)$ coincides with the field of invariants $\mathrm{Quot}(A^G) = \mathrm{Quot}(A)^G$. We also study various localizations and homomorphisms of modular invariant rings as tools to construct generators for A^G. We prove that there is always a nonzero transfer $c \in A^G$ of degree $< |G|$, such that the localization $(A^G)_c$ can be generated by fractions of homogeneous invariants of degrees less than $2 \cdot |G| - 1$. If $A = \mathrm{Sym}(V \oplus \mathbb{F}G)$ with finite-dimensional $\mathbb{F}G$-module V, then c can be chosen in degree one and $2 \cdot |G| - 1$ can be replaced by $|G|$. Let $\mathcal{N}$ denote the image of the classical Noether-homomorphism (see the definition in the paper). We prove that $\mathcal{N}$ contains the transfer ideal and thus can be used to calculate generators for A^G by standard elimination techniques using Gröbner-bases. This provides a new construction algorithm for A^G.

Keywords: Modular invariant theory; Computational algebra; Localization

* Corresponding author.

E-mail addresses: p.fleischmann@kent.ac.uk (P. Fleischmann), kemper@ma.tum.de (G. Kemper), c.f.woodcock@kent.ac.uk (C. Woodcock).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.06.038

1. Introduction

Let K be a field and G be a finite group acting linearly on the polynomial ring $A := K[X_1, \ldots, X_n]$. It is a classical result of Emmy Noether that the ring of invariants $A^G := \{f \in A \mid g(f) = f,\ \forall g \in G\}$ is a finitely generated algebra. If K has characteristic zero or $p > 0$ not dividing the group order $|G|$, then it is known that A^G can be generated by invariants of degree less than or equal to $|G|$ (see [7,10,12]), which is called the *Noether-bound* for the degrees of generators of A^G. If K has characteristic $p > 0$ dividing $|G|$, then in general the Noether bound does not hold (see [15]), however, as we show in Section 2 below, it still holds for the field of invariants $\mathrm{Quot}(A^G)$.

This result is the starting point for a further investigation of degree bounds for various localizations of A^G, which will lead to a proof of the fact that there always exists a nonzero invariant $c \in A^G$ of degree less than $|G|$ such that if C is the subalgebra of A^G, generated by all homogeneous invariants of degree less than or equal to $2|G| - 1$, then the localizations C_c and $(A^G)_c$ coincide. This is remarkable in the light of the fact that for the ring A^G one cannot expected a degree bound depending only on the group order $|G|$ (see [15]).

However, the main motivation for studying these localizations of A^G is derived from the following observation: Let $B \leqslant A^G$ be a "constructible" subalgebra which happens to have the same quotient field as A^G. If moreover A^G is a finite B-module, then we are almost "one step short" of constructing A^G itself. Indeed, in this situation there exists a nonzero "conductor-element" $c \in B$ such that $cA^G \subseteq B$ hence $A^G = c^{-1}(cA \cap B)$ (see 3.3, 3.5). As we will see in 3.6 and 3.7, the required computations that lead to a set of algebra generators for A^G can be performed by standard elimination techniques using Gröbner-bases, as described for example in [5] or [1].

The paper is organized as follows:

In Section 2 we introduce some notation and prove the Noether bound for fields of invariants in arbitrary characteristic. In Section 3, we introduce the concept of the conductor to a subalgebra and describe a general framework of how to use it to generate A^G. We also give some criteria on how to decide whether a given subalgebra is in fact the full ring of invariants.

In Section 4 we describe, still in fairly general terms, the interplay between certain homomorphisms of invariant rings and their localizations. We show that in certain circumstances we can construct subalgebras B that contain the image of the transfer t_1^G. As a consequence any nonzero element $c \in t_1^G(A)$ will lie in the conductor of B. Moreover we show that a suitable c can be found in degree less than $|G|$, in such a way that the localization A_c^G is generated in degree $2|G| - 1$.

Section 5 investigates the classical Noether-homomorphism from vector invariants of symmetric groups to arbitrary rings of invariants. This homomorphism was used in one of the original proofs of Emmy Noether for the degree bound in characteristic zero, that bears her name. Here in the modular situation it turns out that the image $\mathcal{N}$ of the Noether homomorphism contains the image of the transfer and therefore provides a subalgebra satisfying all the necessary hypotheses described in the earlier sections.

In Section 6 we restrict to the case of p-groups over the prime field $\mathbb{F}_p$ and describe a relation of A^G to a new type of "reciprocal invariants" discovered and studied by one of the authors. This ring of reciprocal invariants is generated in negative degrees, bounded only

by the dimension of the underlying group representation, independently of G. Nevertheless it shares a common localization with A^G. Although the degree bound for this localization is weaker than the ones obtained earlier, the "exceeding degrees" are accounted for by invariants which are explicitly described and very well understood. In some applications there can be reason to sacrifice some unknown low degree invariants and rather stick with "known devils" of higher degree.

2. Invariant fields

Suppose that K is a field and $L = K(a_1, \ldots, a_n)$ is a finitely generated field extension. As a typical example, L may be a rational function field in n indeterminates. Let G be a finite group consisting of automorphisms of L which fix K element-wise. The following construction gives an easy method for constructing generators of the invariant field L^G. This method only involves arithmetic in a polynomial ring over L. Take two indeterminates T and U, and form the polynomial

$$F(T,U) := \prod_{g\in G}\left(T - \sum_{i=1}^{n} U^{i-1} g(a_i)\right) \in L^G[T,U].$$

Moreover, for each $i = 1, \ldots, n$ form

$$H_i(T) := \prod_{a\in Ga_i} (T - a) \in L^G[T],$$

where Ga_i denotes the G-orbit of a_i.

Theorem 2.1. *In the above situation, let $M \subseteq L^G$ be the set consisting of all coefficients of $F(T,U)$ and of the $H_i(T)$. Then M generates L^G as a field extension of K.*

If K is of characteristic 0, it suffices to take all coefficients of $F(T,U)$ into M, so the polynomials $H_i(T)$ are unnecessary.

Proof. Write $N := K(M)$ for the field extension generated by M. We clearly have $N \subseteq L^G$. To prove the converse, first consider the case $\operatorname{char}(K) = 0$, so M consists of the coefficients of $F(T,U)$ only. For each $u \in K$ we have

$$F(T,u) = \prod_{g\in G}\left(T - \sum_{i=1}^{n} u^{i-1} g(a_i)\right) \in N[T], \tag{1}$$

so $\sum_{i=1}^{n} u^{i-1} a_i$ is algebraic over N. Choose n distinct elements $u_1, \ldots, u_n \in K$ and set $b_j := \sum_{i=1}^{n} u_j^{i-1} a_i$. Then by the Vandermonde determinant we have $K(b_1, \ldots, b_n) = K(a_1, \ldots, a_n) = L$, hence also $L = N(b_1, \ldots, b_n)$. With (1) it follows that L is the splitting field of $\prod_{i=1}^{n} F(T, u_i)$ over N. Since all field extensions in characteristic 0 are separable, we obtain that L is a finite Galois extension of N.

Now assume that K has positive characteristic and the coefficients of the $H_i(T)$ are included in M. Then $L = N(a_1, \ldots, a_n)$ is the splitting field of $\prod_{i=1}^{n} H_i(T)$ over N and thus a finite normal extension of N. Since $H_i(T)$ has pairwise distinct roots, each a_i is separable over N, so the extension L is separable as well. As in the case of characteristic 0, we obtain that L is a finite Galois extension of N.

In both cases, let H be the Galois group. Clearly $G \subseteq H$, since G consists of automorphism of L fixing N. To prove the reverse inclusion, take $\sigma \in H$ arbitrary. Since all coefficients of $F(T, U)$ lie in N, we have $\sigma(F(T, U)) = F(T, U)$, where we set $\sigma(T) := T$ and $\sigma(U) := U$. Thus

$$\prod_{g\in G}\left(T - \sum_{i=1}^{n} U^{i-1} g(a_i)\right) = \prod_{g\in G}\left(T - \sum_{i=1}^{n} U^{i-1}\sigma\big(g(a_i)\big)\right).$$

We have $\sum_{i=1}^{n} U^{i-1}\sigma(a_i) \in L[U]$ as a zero of the right-hand side, hence there exists a $g \in G$ with

$$\sum_{i=1}^{n} U^{i-1}\sigma(a_i) = \sum_{i=1}^{n} U^{i-1} g(a_i).$$

This implies $\sigma(a_i) = g(a_i)$ for all i, so $\sigma = g \in G$. We obtain $H = G$, so $L^G = L^H = N$ by Galois theory. □

We can derive a degree bound for the invariant field from Theorem 2.1. Before we formulate it, we fix some notation which will be used throughout the paper. Let R be a commutative ring, $A := R[a_1, a_2, \ldots, a_n]$ a finitely generated R-algebra with set of generators $\mathbf{a} := \{a_1, \ldots, a_n\}$ and G a finite group acting on A by R-algebra automorphisms, stabilizing the R-module $\sum_{i=1}^{n} Ra_i$. We define the ring of G-invariants $A^G := \{a \in A \mid g(a) = a,\ \forall g \in G\}$.

For $\gamma \in \mathbb{N}_0^n$ we define the power product $\mathbf{a}^\gamma := \prod_{i=1}^{n} a_i^{\gamma_i}$ and $|\gamma| := \sum_{i=1}^{n} \gamma_i$.

Definition 2.2 *(Noether numbers for quotient fields).* Assume that A is a domain and let $C \leqslant A$ be an R-subalgebra. Let

$$\mathcal{M}_m(\mathbf{a}) := \sum_{\alpha\in\mathbb{N}_0^n,\ |\alpha|\leqslant m} R \cdot \underline{a}^\alpha.$$

We define for the quotient field $\mathrm{Quot}(C)$:

$$\begin{aligned}\beta\big(\mathrm{Quot}(C)\big) &:= \beta\big(\mathrm{Quot}(C), C, \mathbf{a}\big)\\ &:= \min\big\{k \in \mathbb{N}_0 \mid \mathrm{Quot}\big(R\big[C \cap \mathcal{M}_k(\mathbf{a})\big]\big) = \mathrm{Quot}(C)\big\}.\end{aligned}$$

The following corollary states that the classical Noether bound holds for invariant fields. Note that for invariant rings the Noether bound only holds if the characteristic of the ground

field does not divide the group order (see [7,10,15]). In contrast, the corollary holds in arbitrary characteristic.

Corollary 2.3. *In the above situation, let A be a domain. Then*

$$\beta\big(\mathrm{Quot}\big(A^G\big), \mathbf{a}\big) \leqslant |G|.$$

Proof. Let H be the image of G under the map $G \to \mathrm{Aut}(A)$ induced by the action of G. Then $A^G = A^H$ and $|H| \leqslant |G|$. Hence we may assume that $G = H$ is a group consisting of automorphisms of A. With $L = \mathrm{Quot}(A)$ and $K = \mathrm{Quot}(R)$, we obtain that L^G is generated by the set M of Theorem 2.1. Since the G-action preserves the R-module $\sum_{i=1}^n Ra_i$, it follows from the construction of M that all elements from M lie in $A^G \cap \mathcal{M}_{|G|}(\mathbf{a})$. (In fact, it suffices to assume that G stabilizes $R + \sum_{i=1}^n Ra_i$, i.e., every a_i is mapped to a constant plus a linear combination of the a_j.) So

$$L^G = K(M) = \mathrm{Quot}\big(R[M]\big) \subseteq \mathrm{Quot}\big(R\big[A^G \cap \mathcal{M}_{|G|}(\mathbf{a})\big]\big) \subseteq L^G.$$

Finally $L^G = \mathrm{Quot}(A^G)$. This is well known and follows from the fact that every $f/h \in L^G$ with $f, h \in A$ can be written as

$$f/h = \frac{f \cdot \prod_{g \in G \setminus \{\mathrm{id}\}} g(h)}{\prod_{g \in G} g(h)} \in \mathrm{Quot}\big(A^G\big). \qquad \square$$

Let B be a domain and a finitely generated R-algebra, $C \leqslant B$ a subalgebra and assume that $\mathrm{Quot}(C) = \mathrm{Quot}(B)$. Then it is easy to see that there is a single element $0 \neq c \in C$ such that

$$C_c := C[1/c] = B[1/c] = B_c.$$

In the above situation it is known by a result of E. Noether [13], A^G is finitely generated, if R is Noetherian. Taking $C := R[A^G \cap \mathcal{M}_{|G|}(\mathbf{a})]$ we get:

Corollary 2.4. *Assume that R is Noetherian and A is a domain. Then there exists $c \in A^G \setminus \{0\}$ such that*

$$R\big[A^G \cap \mathcal{M}_{|G|}(\mathbf{a})\big]_c = A_c^G.$$

Note that unlike Theorem 2.1 and Corollary 2.3, which are completely constructive, the result in this corollary is not constructive. In particular, it provides no method for finding an element c with the described property or any degree bound for such a c. In the sequel we will find degree bounds and more explicit constructions for such elements c. However, the price we have to pay for this is that in most cases we have to make compromises in the quality of our degree bound. In fact, the general bound will be $2|G| - 1$ instead of $|G|$.

We will use the following

Definition 2.5 *(Noether numbers for subrings and localizations).* For an R-subalgebra $C \leqslant A$ and $0 \neq c \in C$ we define

$$\beta(C_c) := \beta(C, c, \mathbf{a}) := \min\bigl\{k \in \mathbb{N}_0 \mid c \in \mathcal{M}_k(\mathbf{a}),\ C_c = R\bigl[C \cap \mathcal{M}_k(\mathbf{a}), 1/c\bigr]\bigr\}.$$

3. Subrings and conductors

In the rest of this paper, unless explicitly stated otherwise, all rings considered are assumed to be domains.

Definition 3.1. Let $B \leqslant A \subseteq \mathrm{Quot}(A)$ be domains. The set

$$\mathcal{C}(B, A) = [B : A]_A := \{c \in A \mid cA \subseteq B\}$$

is called the *conductor* of A into B. We also define

$$\mathcal{T}(B, A) := \bigl\{b \in B \setminus \{0\} \mid bA \cap B = bB\bigr\}.$$

We have

Lemma 3.2.

(1) $\mathcal{C}(B, A) = \{b \in B \mid b^{-1}B \cap A = A\} \cup \{0\}$ *is the largest ideal in A which is contained in B.*
(2) $\mathcal{T}(B, A) := \{b \in B \setminus \{0\} \mid b^{-1}B \cap A = B\}$ *is the largest multiplicative subset S of B with $B_S \cap A = B$.*
(3) *The following are equivalent*:
  (i) $A = B$;
  (ii) $\mathcal{T}(B, A) \cap \mathcal{C}(B, A) \neq \emptyset$;
  (iii) $\mathcal{C}(B, A) = A$;
  (iv) $\mathcal{T}(B, A) = B \setminus \{0\}$ *and* $\mathcal{C}(B, A) \neq 0$.

Proof. (1) is obvious.

(2) Let $b, b' \in \mathcal{T}(B, A)$ and $a \in A$ with $x := bb'a = b(b'a) \in B$. Then $bb'a = bb''$ with $b'' \in B$, hence $b'a = b'' \in b'A \cap B$, so $b'a = b'\tilde{b}$ with $\tilde{b} \in B$ and $a = \tilde{b}$. It follows that $x = bb'\tilde{b} \in bb'B$, so $bb'A \cap B = bb'B$ and $bb' \in \mathcal{T}(B, A)$. This shows that $T := \mathcal{T}(B, A)$ is multiplicative with $B_T \cap A = B$. On the other hand, if $S \subseteq B$ is multiplicative with $B_S \cap A = B$, then clearly $S \subseteq T$.

(3) "(ii) $\Rightarrow$ (i)," "(i) $\Rightarrow$ (iii)" and "(iii) $\Rightarrow$ (ii)" are obvious (note that $1 \in \mathcal{T}(B, A)$). But also "(i) $\Rightarrow$ (iv)" and "(iv) $\Rightarrow$ (ii)" are clear. □

Theorem 3.3. *Let $A = B[a_1, \ldots, a_k]$ and B be Noetherian, then the following are equivalent*:

(1) $\mathcal{C}(B, A) \neq 0$.
(2) $\mathrm{Quot}(B) = \mathrm{Quot}(A)$ *and A is integral over B.*

Proof. "(1) $\Rightarrow$ (2)" Let $0 \neq c \in \mathcal{C} := \mathcal{C}(B, A)$. Then $cA \subseteq B$, hence $A_c \subseteq B_c$, so $\mathrm{Quot}(A) = \mathrm{Quot}(B)$. Now take $c \in \mathcal{C}(B, A) \setminus 0$. Then cA is an ideal in B and therefore a finitely generated B-module. But $c \in B$, so cA is isomorphic to A as a B-module. Thus A is a finitely generated B-module, so A is integral over B.

"(1) $\Leftarrow$ (2)" Since A is integral over B, A is a finitely generated B-module, say generated by $e_1, \ldots, e_k$. Since $\mathrm{Quot}(B) = \mathrm{Quot}(A)$, we have $e_j = u_j/v_j$ with $u_j, v_j \in B$ and clearly the product $0 \neq v_1 v_2 \cdots v_k$ is contained in $\mathcal{C}$. □

For $n \in \mathbb{N}$ and an R-subalgebra $B \leqslant A$, define $B_{[n]} := R[B \cap \mathcal{M}_n(\mathbf{a})]$. If R is a field, $V \in RG - \mathrm{mod}$ and $A := \mathrm{Sym}(V^*)$ with $\{a_i \mid 1 \leqslant i \leqslant n\}$ being a basis of V^*, then

$$\prod_{g \in G} \big(T - g(a_i)\big) \in A^G_{[|G|]}[T],$$

hence A^G is integral over any $B \leqslant A^G$ containing $A^G_{[|G|]}$. We get:

Corollary 3.4. *Let $A := \mathrm{Sym}(V^*)$, $m := |G|$ and $A^G_{[m]} \leqslant B \leqslant A^G$. Then $\mathcal{T}(B, A) = \mathcal{T}(B, A^G)$ and $\mathcal{C}(B, A^G) \neq 0$.*

Proof. Let $b \in B \setminus \{0\}$. Since $b^{-1}B \cap A = b^{-1}B \cap A^G$, Lemma 3.2(2) shows $\mathcal{T}(B, A) = \mathcal{T}(B, A^G)$. Since A^G is integral over B, the fact that $\mathcal{C}(B, A^G) \neq 0$ follows from 3.3 together with 2.3. □

The significance of 3.4 and the importance of knowing nonzero elements in the conductor can be seen as follows: We are in precisely one of the following situations:

(1) either $\mathcal{T}(B, A) = B \setminus \{0\}$ in which case $B = A^G$,
(2) or $\exists b \in (B \setminus \{0\}) \setminus \mathcal{T}(B, A)$, in which case

$$B \subsetneqq b^{-1}(bA \cap B) = A^G \cap b^{-1}B \subseteq A^G.$$

This means that a "new invariant" b' can be obtained, dividing a suitable element of $bA \cap B$ by b.
(3) Setting $B' := B[b']$ we can go to (1) and iterate.

Since $B < B' \leqslant A^G$ are B-submodules of the Noetherian B-module A^G this process must terminate with A^G. However, it would not be justified to call the method sketched here an "algorithm" since it is not clear how $\mathcal{T}(B, A)$ can be calculated algorithmically. Note that $bA \cap B = bA^G \cap B$, so the calculations can in principle be done without knowing A^G. Moreover, finding a nonzero element in the conductor $\mathcal{C}(B, A^G)$ brings us one step short of calculating generators for A^G:

Proposition 3.5. *Let $0 \neq c \in \mathcal{C}(B, A^G)$, and $b_1, \ldots, b_t \in B$ generators of the ideal $cA \cap B \trianglelefteqslant B$. Define $[B : c]_A := \{a \in A \mid ac \in B\}$, then $b'_i := b_i/c \in A^G$ for $i = 1, \ldots, t$ and*

$$A^G = [B : c]_A = c^{-1}(cA \cap B) = \sum_{i=1}^{t} Bb'_i = B\big[b'_1, \ldots, b'_t\big].$$

Proof. Since

$$cA \cap B = cA^G \cap B = cA^G = \sum_{i=1}^{t} Bb_i \trianglelefteqslant B,$$

the element c divides every b_i in A and A^G. Hence $b'_i \in A^G$ and the result follows. □

Assume that $\mathbb{F} = R$ is a field and $A = \mathbb{F}[a_1, \ldots, a_n]$ is a finitely generated algebra. Once the subalgebra algebra B and the element $0 \neq c \in \mathcal{C}(B, A^G)$ are given, the intersection $cA \cap B$ can be calculated by standard elimination techniques using Gröbner bases. The following is a variation of [5, Proposition 15.30]:

Proposition 3.6. *Let $A = \mathbb{F}[Y_1, \ldots, Y_n]/I$ with ideal $I \trianglelefteqslant \mathbb{F}[Y_1, \ldots, Y_n]$ and subalgebra $B := \mathbb{F}[f_1, \ldots, f_m] \leqslant A$, where $f_j := F_j(a_1, \ldots, a_n)$ with $a_i := Y_i \bmod (I)$ and $F_j \in \mathbb{F}[Y_1, \ldots, Y_n]$. Let $C \in \mathbb{F}[Y_1, \ldots, Y_n]$ and set $c := C(a_1, \ldots, a_n) \in A$. Now consider the polynomial ring $T := \mathbb{F}[Y_1, \ldots, Y_n, Z_1, \ldots, Z_m]$, form the ideal $J \trianglelefteqslant T$, generated by I, C and all $F_j - Z_j$ and let $\mathcal{E}$ be the elimination ideal $J \cap \mathbb{F}[Z_1, \ldots, Z_m]$.*

If Ψ is the epimorphism of algebras

$$\Psi : T \to A, \quad Y_i \mapsto a_i, \quad Z_j \mapsto f_j,$$

then $\ker(\Psi) = (I, F_j - Z_j \mid j = 1, \ldots, m)T$, $\Psi(\mathbb{F}[Z_1, \ldots, Z_m]) = B$, $\Psi(J) = cA$ *and*

$$\Psi(\mathcal{E}) = cA \cap B.$$

In particular, substituting $Z_i \mapsto f_i$ in each generator of $\mathcal{E}$ yields generators for $cA \cap B$.

Proof. Clearly $\mathcal{R} := (I, F_j - Z_j \mid j = 1, \ldots, m)T \leqslant \ker(\Psi)$. Let $\lambda(\mathbf{Y}, \mathbf{Z}) \in \ker(\Psi)$, then $\lambda(\mathbf{Y}, F_1(\mathbf{Y}), \ldots, F_m(\mathbf{Y})) \in I$ and

$$\lambda(\mathbf{Y}, \mathbf{Z}) - \lambda\big(\mathbf{Y}, F_1(\mathbf{Y}), \ldots, F_m(\mathbf{Y})\big) \in (F_j - Z_j \mid j = 1, \ldots, m)T,$$

so $\lambda(\mathbf{Y}, \mathbf{Z}) \in \mathcal{R}$ and $\ker(\Psi) = \mathcal{R}$. It is clear that $\Psi(J) = cA$, $\Psi(\mathbb{F}[Z_1, \ldots, Z_m]) = B$ and $\Psi(\mathcal{E}) \subseteq cA \cap B$. Let $\chi = \Psi(f) = \Psi(h(\mathbf{Z}))$ with $f \in J$ and $h \in \mathbb{F}[Z_1, \ldots, Z_m]$. Then $h(\mathbf{Z}) = f + h(\mathbf{Z}) - f \in f + \ker(\Psi) \subseteq J$, so $h(\mathbf{Z}) \in \mathcal{E}$ and $\Psi(\mathcal{E}) = cA \cap B$. □

Remark 3.7. The calculation of generators for the elimination ideal $\mathcal{E} = J \cap \mathbb{F}[Z_1, \ldots, Z_m]$ is a standard application of Gröbner bases, hence 3.6 provides an algorithm to calculate generators for A^G, once a subalgebra $B \leqslant A^G$ and an element $0 \neq c \in \mathcal{C}(B, A^G)$

are known. In 4.1 and 5.4 we will consider situations where suitable subalgebras B and nonzero conductor elements arise.

The following lemma gives two further conditions for $B = A^G$, one of them is in terms of the grade of $\mathcal{C}(B, A^G)$ acting on B. Recall that for an ideal $I \trianglelefteq R$ of a ring R and an R-module M with $IM \subsetneqq M$ the grade, $\operatorname{grade}(I, M)$ is defined to be the maximal length of a regular M-sequence inside I. If $M = IM$, then $\operatorname{grade}(I, M) := \infty$ (see [3, Definition 1.2.6]).

Proposition 3.8. *Let $B \leqslant A^G$ and assume $C := \mathcal{C}(B, A^G) \neq 0$.*

(1) $A^G = B \Leftrightarrow \operatorname{grade}(C, B) \geqslant 2$.
(2) *If $\sqrt{C}$ contains a nonzero principal radical ideal of B, i.e. an ideal $0 \neq bB = \sqrt{bB}$, then $B = A^G$.*

Proof. (1) "$\Rightarrow$" follow from the definition of grade, since in this case $C = B$. "$\Leftarrow$" first assume that $CB = B$; then $1 \in B = CB = C$, hence $A^G = CA^G \subseteq B \subseteq A^G$. Now assume $CB \subsetneqq B$, let (c, c') be a regular sequence in C on B and let $a \in A^G$. Then $ca = b \in B$ the equation $c'b = cc'a$ implies that $b = cb'$ for some $b' \in B$. Hence $a = b' \in B$.

(2) Suppose $0 \neq bB = \sqrt{bB} \subseteq \sqrt{C}$. Then $b^N A^G \subseteq B$ for some $N > 0$. Hence

$$\left(bA^G \cap B\right)^{N+1} \subseteq bb^N A^G \subseteq bB.$$

It follows that $bA^G \cap B = bB$, so $b \in \mathcal{T}(B, A^G)$ and $b^N \in \mathcal{T}(B, A^G) \cap C$. The result follows from 3.2. □

4. Homomorphisms and localization

In the last section we have seen the importance of constructing subalgebras $B \leqslant A^G$ with $\operatorname{Quot}(B) = \operatorname{Quot}(A^G)$ and explicit nonzero elements in the conductor $\mathcal{C}(B, A^G)$. In this section we describe a generic situation in which this can be achieved. The results obtained here will later be applied in a more specialized case (see 5.4). From now on we will always assume that G acts faithfully on A.

Let $H \leqslant G$ be a subgroup of index m and $G := \bigcup_{i=1}^{m} g_i H$ the coset decomposition. Assume that A^H is known and consider the *relative transfer map* with respect to H:

$$t_H^G : A^H \to A^G, \quad a \mapsto \sum_{i=1}^{m} g_i(a).$$

This is an A^G-module homomorphism and the image $t_H^G(A^G)$ is an ideal in A^G, called the *relative transfer ideal* (w.r.t. H). This ideal plays an important role in the construction of A^G by "transferring H-invariants into G-invariants."

Let $\tilde{G}$ be a finite group, $\theta : G \to \tilde{G}$ a group homomorphism and B an R-algebra on which $\tilde{G}$, and hence G, act by R-algebra automorphisms. Let $\nu : B \to A$ be a G-equivariant homomorphism of R-algebras; then clearly $\nu(B^G)$ is a subalgebra of A^G, which in general will be a proper inclusion, even if $\nu(B) = A$.

However the algebras $\nu(B^G)$ and A^G are still closely related: it turns out that the quotient fields $\mathrm{Quot}(A^G)$ and $\mathrm{Quot}(\nu(B^G))$ coincide and A^G is purely inseparable over $\nu(B^G)$. For the subalgebra $C \leqslant A$ and $n \in \mathbb{N}$ let $\sqrt[n]{C} := \{a \in A \mid a^n \in C\}$.

Theorem 4.1. *For $\tilde{H} \leqslant \tilde{G}$, a subgroup of index $m = [G : H]$, assume that $\nu(B^{\tilde{H}}) = A^H$ and $\tilde{G} = \bigcup_{i=1}^{m} \theta(g_i) \cdot \tilde{H}$. Then*

(1) *$t_H^G(A^H) = \nu(t_{\tilde{H}}^{\tilde{G}}(B^{\tilde{H}})) \trianglelefteqslant A^G$ is a nonzero ideal of A^G, contained in the subalgebras $\nu(B^{\tilde{G}}) \leqslant \nu(B^G) \leqslant A^G$. In particular*

$$t_H^G\big(A^H\big) \subseteq \mathcal{C}\big(\nu\big(B^{\tilde{G}}\big), A^G\big) \subseteq \mathcal{C}\big(\nu\big(B^G\big), A^G\big).$$

(2) *For every $0 \neq c \in t_H^G(A^H)$ we have for the localizations*:

$$\nu\big(B^{\tilde{G}}\big)_c = \nu\big(B^G\big)_c = \big(A^G\big)_c.$$

In particular, $\mathrm{Quot}(A^G) = \mathrm{Quot}(\nu(B^G)) = \mathrm{Quot}(\nu(B^{\tilde{G}}))$.

(3) *Now assume that $\mathbb{F}_p \subseteq R$ and let p^r be the maximal p-power dividing m. Then $\sqrt[p^r]{\nu(B^G)} = A^G$, i.e. for every $f \in A^G$, $f^{p^r} \in \nu(B^G)$.*

Proof. (1) The field extension $\mathrm{Quot}(A) : \mathrm{Quot}(A)^G$ is Galois' with $\mathrm{Quot}(A)^G = \mathrm{Quot}(A^G)$. By standard Galois theory the trace map $t_1^G : \mathrm{Quot}(A) \to \mathrm{Quot}(A)^G$ is surjective. In particular there is $r \in A$ and $0 \neq s \in A^G$ such that $t_1^G(r/s) = 1$, or equivalently, $t_1^G(r) = t_H^G(t_1^H(r)) = s \neq 0$. This shows that $t_H^G(A^H)$ is nonzero. The rest of 1. is obvious, since ν is G-equivariant (with the $\theta(G)$-operation on B), and $\nu(B^{\tilde{H}}) = A^H$.

(2) Let $0 \neq c \in t_H^G(A^H)$, then we have by (1):

$$cA^G \subseteq t_H^G\big(A^H\big) \subseteq \nu\big(B^{\tilde{G}}\big) \subseteq \nu\big(B^G\big) \subseteq A^G.$$

Hence $(A^G)_c = \nu(B^{\tilde{G}})_c = \nu(B^G)_c$ and

$$\mathrm{Quot}(A)^G = \mathrm{Quot}\big(\big(A^G\big)_c\big) = \mathrm{Quot}\big(\nu\big(B^{\tilde{G}}\big)_c\big) = \mathrm{Quot}\big(\nu\big(B^{\tilde{G}}\big)\big).$$

(3) Let $m = p^r s$ with $\gcd(p, s) = 1$, let Q be a Sylow p-group of H and P a Sylow p-group of G containing Q. Let $f \in A^G$; by the hypothesis there is $b \in B^H$ with $\nu(b) = f$. Define $\eta := \prod_{g \in P/Q} g(b) \in B^P$. Then

$$\nu\big(t_P^G(\eta)\big) = \sum_{x\in G/P} \nu(x\eta) = \sum_{x\in G/P} x\Big(\nu\Big(\prod_{g\in P/Q} g(b)\Big)\Big)$$
$$= \sum_{x\in G/P} x\Big(\prod_{g\in P/Q} g\nu(b)\Big) = \sum_{x\in G/P} x\big(\nu(b)^{p^r}\big) = [G:P]\cdot \nu(b)^{p^r}.$$

Hence $f^{p^r} \in \nu(B^G)$. □

In the situation of 4.1 let $K := \ker\ \nu$. The short exact sequence $0 \to K \to B \to A \to 0$ of B^G-modules induces the exact sequence

$$0 \to K^G \to B^G \to A^G \to H^1(G, K),$$

with $\delta : A^G \to H^1(G, K)$ a connecting homomorphism. In particular the algebras $B^{\tilde{G}} \leqslant B^G$ act on $H^1(G, K)$ in a natural way. Clearly $A^G = \nu(B^G)$, if and only if δ is the zero map, for example, if $H^1(G, K) = 0$. The following is a slightly sharper criterion in terms of grades of relative transfer ideals acting on $H^1(G, K)$:

Proposition 4.2. *Assume that*

$$\operatorname{grade}\big(t_H^G\big(B^H\big), H^1(G, K)\big) \geqslant 1, \quad \text{or} \quad \operatorname{grade}\big(t_{\tilde{H}}^{\tilde{G}}\big(B^{\tilde{H}}\big), H^1(G, K)\big) \geqslant 1.$$

Then $\nu(B^G) = A^G$.

Proof. Let $\mathcal{I} := t_H^G(B^H)$, $\mathcal{J} := t_{\tilde{H}}^{\tilde{G}}(B^{\tilde{H}})$ and assume that $0 \neq t \in \mathcal{I} \cup \mathcal{J}$ is regular on $H^1(G, K)$. Note that by the hypotheses of 4.1, we have $\nu(B^H) \subseteq A^H = \nu(B^{\tilde{H}})$, hence

$$\nu\big(t_H^G\big(B^H\big)\big) = t_H^G\big(\nu\big(B^H\big)\big) \subseteq t_H^G\big(\nu\big(B^{\tilde{H}}\big)\big) = \nu\big(t_{\tilde{H}}^{\tilde{G}}\big(B^{\tilde{H}}\big)\big) = t_H^G\big(A^H\big).$$

Since $A^G/\nu(B^G) = \operatorname{Im}\delta$ and t acts on this quotient as $\nu(t)$, 4.1 implies that $t(\operatorname{Im}\delta) = 0$, hence $\operatorname{Im}\delta = 0$ and therefore $\nu(B^G) = A^G$. □

Obviously we have $\beta(\operatorname{Quot}(A^G), \mathbf{a}) \leqslant \beta(A^G, \mathbf{a})$ and in general this will be a strict inequality. If $B = R[b_1, \ldots, b_n]$ and A are domains with $\nu : B \to A$ a G-equivariant R-algebra epimorphism, then 4.1 shows:

Corollary 4.3. $\beta(\operatorname{Quot}(A^G), \nu(\mathbf{b})) \leqslant \beta(B^G, \mathbf{b})$.

Remark 4.4. Let $R = \mathbb{F}$ be a field and $A = \operatorname{Sym}(V^*)$ with $V^* = \langle v^G\rangle$, where v^G denotes the G-orbit of v. If $|v^G| =: t$, then we can take $B := \mathbb{F}[X_{gv} \mid gv \in v^G]$ with $\nu : B \to A$ defined by $X_{gv} \mapsto gv$. Using Göbel's degree bound for permutation invariants [11] this implies

$$\beta\big(\operatorname{Quot}\big(A^G\big)\big) \leqslant \beta\big(B^G\big) \leqslant \binom{t}{2}.$$

If R is $\mathbb{Z}$ or a field of characteristic p dividing $|G|$, one knows that general degree bounds $\beta(A^G)$ cannot depend only on $|G|$. For A a polynomial ring the following degree bound is conjectured to hold (see [4, 3.9.10]):

$$\beta\big(A^G\big) = \max\big\{|G|, \operatorname{Dim}(A)\big(|G|-1\big)\big\}. \tag{2}$$

However for the quotient field $\operatorname{Quot}(A^G)$ the Noether bound still holds (see 2.3). It also turns out that the localization of A^G at a single suitable invariant, in fact a nonzero transfer element of degree $\leqslant |G|$, satisfies at least a 'global degree bound' close to the Noether bound. To see this we need the following lemma, which describes a decomposition, *in the ambient ring* A, of high "degree" relative transfer elements.

For the next two lemmas, R and A can be arbitrary commutative rings. The following lemma is in fact a corollary to the Fogarty and Benson's proof of the Noether-bound in the coprime case (see [10]):

Lemma 4.5. *Let* $\underline{m} := \{1, 2, \ldots, m\}$. *For* $b, b_1, b_2, \ldots, b_m \in A^H$ *we have*

$$t_H^G(bb_1\cdots b_m) = \sum_{I\subset \underline{m},\, I\neq \underline{m}} (-1)^{m-|I|+1}\, t_H^G\Big(b\prod_{j\in I} b_j\Big) \prod_{j\in \underline{m}\setminus I} g_j(b_j).$$

Proof. We consider the obvious equality for fixed i:

$$\prod_{j=1}^{m}\big(g_i(b_j) - g_j(b_j)\big) = 0.$$

Expansion and multiplication with $g_i(b)$ for fixed i gives:

$$0 = \sum_{I\subseteq \underline{m}} (-1)^{m-|I|}\Big(\prod_{j\in \underline{m}\setminus I} g_j(b_j)\Big)\cdot\Big(\prod_{j\in I} g_i(b_j)\Big)\cdot g_i(b).$$

Now summation over $i \in \underline{m}$ yields the claimed identity. □

Definition 4.6. For $A = R[a_1, \ldots, a_n]$ we define $\delta(A^G, \mathbf{a})$ to be the minimal number $k \in \mathbb{N}_0$ such that there is a power product $f := \mathbf{a}^\gamma$ with $|\gamma| = \sum_{i=1}^n \gamma_i = k$ and $t_1^G(f) \neq 0$.

Lemma 4.7. *If* $t_1^G(A) \neq 0$, *then* $\delta(A^G, \mathbf{a}) \leqslant |G| - 1$.

Proof. Assume otherwise. Then 4.5 shows for $H = 1$, $A = R[a_1, \ldots, a_n]$, $m := |G|$, $b = 1$ and $b_1, b_2, \ldots, b_m \in A$:

$$t_1^G(b_1\cdots b_m) = \sum_{I\subset \underline{m},\, I\neq \underline{m}} (-1)^{m-|I|+1} t_1^G\Big(\prod_{j\in I} b_j\Big) \prod_{j\in \underline{m}\setminus I} g_j(b_j).$$

An obvious iteration yields the contradiction $t_1^G(A) = 0$. □

Theorem 4.8. *Let $m = |G|$ and $A = R[a_1, \dots, a_n]$ be a domain. Then $\delta := \delta(A^G, \mathbf{a}) \leqslant m - 1$ and for every $f \in \mathcal{M}_\delta(\mathbf{a})$ with $0 \neq c := t_1^G(f)$ one has*:

$$\big(A^G\big)_c = R\big[A^G \cap \mathcal{M}_{m+\delta}(\mathbf{a}), 1/c\big],$$

hence $\beta(A_c^G, \mathbf{a}) \leqslant \delta + |G| \leqslant 2 \cdot |G| - 1$.

Proof. Let $D := R[A^G \cap \mathcal{M}_{\delta+m}(\mathbf{a}), 1/c]$. Since A is a domain, $t_1^G(A) \neq 0$ by 4.1, hence there is $c := t_1^G(f) \neq 0$ with f as in 4.7. Define $\mathcal{R} : A_c \to (A^G)_c$, $x \mapsto 1/c \cdot t_1^G(fx)$. Then $\mathcal{R}$ is a 'Reynolds-operator,' i.e. an A_c^G-linear projection from A_c to A_c^G. Applying $\mathcal{R}$ to the equation in 4.5, we see that for each $\mathfrak{x} \in A$ and $b_1, \dots, b_m \in \{a_1, \dots, a_n\}$:

$$t_1^G(\mathfrak{x} \cdot b_1 \cdots b_m) = \sum_{I \subset \underline{m},\, I \neq \underline{m}} (-1)^{m-|I|+1} t_1^G\Bigg(\mathfrak{x} \prod_{j \in I} b_j\Bigg) \cdot \mathcal{R}\Bigg(\prod_{j \in \underline{m} \setminus I} g_j(b_j)\Bigg). \tag{3}$$

Since $\mathcal{R}(\mathcal{M}_m(\mathbf{a})) \subseteq D$ we get

$$cA^G \subseteq t_1^G(A) \leqslant D \leqslant \big(A^G\big)_c,$$

hence $(A^G)_c = D_c = D$. □

Remark 4.9. Let R be a field of characteristic $p > 0$, V an RG-module and G a p-group. Then $t_1^G(V) \neq 0$ if and only if V contains a direct summand which is a free RG-module (e.g. see [9, Lemma 3.2]). Hence it follows from 4.7 and 4.8 that the RG-module $\mathrm{Sym}(V^*)$ always contains a free summand in degree strictly less than $|G|$.

If $\delta(A^G, \mathbf{a}) \leqslant 1$, then the result in 4.8 gives $\beta(A_c^G, \mathbf{a}) \leqslant |G| + 1$. However, there is a refinement of 4.8, which implies the Noether bound in that case:

Theorem 4.10. *Let $m := |G|$, A a domain, $\delta := \delta(A^G, \mathbf{a})$ and $f \in A_\delta$ with $0 \neq c = t_1^G(f)$. Define the norm of f by $N_G(f) := \prod_{g \in G} g(f) \in A^G$. Then*

$$A_c^G = R\big[N_G(f), A^G \cap \mathcal{M}_{m+\delta-1}(\mathbf{a}), 1/c\big].$$

In particular, if $\delta = 1$, i.e. $f \in \langle a_1, a_2, \dots, a_n \rangle_R$, then

$$\beta\big(A_c^G, \mathbf{a}\big) \leqslant |G|.$$

Proof. Using 4.5 with the g_i's replaced by their inverses, we get for arbitrary $b_1, \dots, b_m \in \sum_{i=1}^n Ra_i$:

$$\begin{aligned} &t_1^G(f \cdot b_1 \cdots b_m) \\ &\quad = \sum_{I \subset \underline{m},\, I \neq \underline{m}} (-1)^{m-|I|+1} t_1^G\Bigg(f \prod_{j \in I} b_j\Bigg) \cdot \frac{1}{c} t_1^G\Bigg(f\Bigg(\prod_{j \in \underline{m} \setminus I} g_j^{-1}(b_j)\Bigg)\Bigg) \end{aligned}$$

$$= (-1)^{m+1} t_1^G\Bigg(f\Bigg(\prod_{j=1,\dots,m} g_j^{-1}(b_j)\Bigg)\Bigg)$$
$$+ \text{summands of the form } \frac{1}{c}\cdot t_1^G\big(f\cdot \mathcal{M}_{m-1}(\mathbf{a})\big)\cdot t_1^G\big(f\cdot\mathcal{M}_{m-1}(\mathbf{a})\big)\subseteq A.$$

Hence

$$t_1^G(f\cdot b_1\cdots b_m)$$
$$\equiv (-1)^{m+1} t_1^G\Bigg(g_i^{-1}(b_i)\cdot f\cdot \prod_{\substack{j=1,\dots,m,\\ j\neq i}} g_j^{-1}(b_j)\Bigg) \mod R\big[1/c, A^G\cap \mathcal{M}_{m+\delta-1}(\mathbf{a})\big].$$

Using Eq. (3) in the proof of 4.8 with $\mathfrak{x} := g_i^{-1}(b_i)$ and the $b_1,\dots,b_m$ there replaced by the m factors $g_1^{-1}(b_1)\cdots g_{i-1}^{-1}(b_{i-1})\cdot f\cdot g_{i+1}^{-1}(b_{i+1})\cdots g_m^{-1}(b_m)$ we get:

$$t_1^G\big(g_i^{-1}(b_i)\ g_1^{-1}(b_1)\cdots g_{i-1}^{-1}(b_{i-1})\cdot f\cdot g_{i+1}^{-1}(b_{i+1})\cdots g_m^{-1}(b_m)\big)$$
$$\equiv (-1)^{m+1}\frac{t_1^G(b_i)}{c}\cdot t_1^G\big(fb_1b_2\cdots g_i(f)\cdots b_m\big) \mod R\big[1/c, A^G\cap\mathcal{M}_{m+\delta-1}(\mathbf{a})\big],$$

hence by iteration

$$t_1^G(f\cdot b_1\cdots b_m)\equiv \frac{t_1^G(b_i)}{c}\cdot t_1^G\big(fb_1b_2\cdots g_i(f)\cdots b_m\big)\equiv\cdots$$
$$\equiv \frac{t_1^G(b_1)t_1^G(b_2)\cdots t_1^G(b_m)}{c^m}\cdot N_G(f)\cdot t_1^G(f)$$
$$\equiv 0 \mod R\big[N_G(f), 1/c, A^G\cap\mathcal{M}_{m+\delta-1}(\mathbf{a})\big].$$

Hence

$$A_c^G = \frac{1}{c}t_1^G(fA) = R\big[1/c, N_G(f), A^G\cap\mathcal{M}_m(\mathbf{a})\big].$$

If $f\in\langle a_1,a_2,\dots,a_n\rangle_R$, then $N_G(f)\in A^G\cap\mathcal{M}_m(\mathbf{a})$, which proves the second claim. □

The following result provides cases where the Noether bound for A_c^G can be established via 4.10.

Proposition 4.11. *Let R be a field of characteristic $p>0$ dividing $|G|$, let V be a finite-dimensional RG-module and $A=\mathrm{Sym}(V^*)$ with $a_1,\dots,a_n$ being an R-basis of V^*. Assume that V has a submodule $W\leqslant V$ which is projective and has a nonzero factor module W/U on which G acts trivially.*[1]

[1] This implies that W^* is a direct summand of V^* with $(W^*)^G\neq 0$.

Then $\delta(A^G, \mathbf{a}) = 1$.
(*This is for example the case, if* $V \cong V' \oplus RG$.)

Proof. If $f \in \mathcal{M}_0(\mathbf{a})$, then f is a constant and $t_1^G(f) = |G| \cdot f = 0$, hence $0 < \delta(A^G, \mathbf{a})$. Note that W as well as W^* are projective and injective, hence they both are direct summands of V and V^*, respectively. By the assumption on W, we have $(W^*)^G \neq 0$. Since W^* is projective, there is $\alpha \in \mathrm{End}_R(W^*)$ with

$$t_1^G(\alpha) := \sum_{g \in G} g \circ \alpha \circ g_{|W^*}^{-1} = \mathrm{id}_{W^*}$$

(see [2, 3.6.4]). Now take $0 \neq f \in (W^*)^G$, then

$$\begin{aligned} 0 \neq f = \mathrm{id}_{W^*}(f) &= \sum_{g \in G} g \circ \alpha \circ g^{-1}(f) \\ &= \sum_{g \in G} g \circ \alpha(f) = t_1^G\big(\alpha(f)\big) \in t_1^G\big(\mathcal{M}_1(\mathbf{a})\big). \end{aligned}$$

This shows that $\delta(A^G, \mathbf{a}) = 1$. □

5. The Noether homomorphism

Special types of permutation invariants can be used to construct generators of arbitrary invariant rings, using ideas of Emmy Noether [12]. Of particular interest are the *vector invariants* of symmetric groups, which we will now discuss.

Let $A(k, n)$ be the polynomial ring $R[X_{11}, \ldots, X_{k1}, \ldots, X_{1n}, \ldots, X_{kn}]$ in $k \times n$ variables, Σ_n the symmetric group on n letters and define an action of Σ_n on $A(k, n)$ by extending the permutation action $\sigma(X_{ij}) := X_{i\sigma(j)}$. The corresponding ring of invariants $A(k, n)^{\Sigma_n}$ is usually called the ring of (k-fold) *vector invariants*.

Let $\mathbf{Y} := (Y_1, \ldots, Y_k)$ be a 'vector of variables'; then the multivariate polynomial

$$G(\mathbf{X}_1, \ldots, \mathbf{X}_n; \mathbf{Y}) := \prod_{j=1}^{n} \left(1 + \sum_{i=1}^{k} X_{i,j} Y_i\right) \in A(k, n)^{\Sigma_n}[Y_1, \ldots, Y_k]$$

is called the *Galois-resolvent*. Let $\mathcal{G} \leqslant A(k, n)^{\Sigma_n}$ be the subalgebra generated by the coefficients of $G(\mathbf{X}_1, \ldots, \mathbf{X}_n; \mathbf{Y})$.

Theorem 5.1. *For any domain* R *we have* $\mathrm{Quot}(A(k, n)^{\Sigma_n}) = \mathrm{Quot}(\mathcal{G})$; *in particular* $\beta(\mathrm{Quot}(A(k, n)^{\Sigma_n})) = n$.

Proof. The proof is a slight variation of the proof of 2.3. We replace the H_i there by $f_i := \prod_{k=1}^{n} (T - X_{ik})$ and define M to be the set of coefficients of $G(\mathbf{X}_1, \ldots, \mathbf{X}_n; \mathbf{Y}) \in A(k, n)^{\Sigma_n}[Y_1, \ldots, Y_k]$. For any ring $\mathbb{S}$ and polynomial $F \in \mathbb{S}[Y_1, \ldots, Y_k]$ we denote the

coefficient of F at $\mathbf{Y}^\gamma := Y_1^{\gamma_1}\cdots Y_k^{\gamma_k}$ by $\operatorname{coeff}_{\mathbf{Y}^\gamma}(F)$. We show that M contains the coefficients of the f_i: Indeed, for $1 \leqslant \ell \leqslant n$:

$$\pm\operatorname{coeff}_{T^{n-\ell}}\left(\prod_{j=1}^{n}(T - X_{ij})\right) = e_\ell(X_{i1},\ldots,X_{in}) = \operatorname{coeff}_{T^{n-\ell}}\left(\prod_{j=1}^{n}(T + X_{ij})\right)$$
$$= \operatorname{coeff}_{Y_i^\ell}\left(\prod_{j=1}^{n}(1 + X_{ij}Y_i)\right) = \operatorname{coeff}_{Y_i^\ell}\big(G(\mathbf{X},\mathbf{Y})\big) \in M.$$

Here e_ℓ denotes the ℓth elementary symmetric function. Since M contains the coefficients of the f_i we have that $\mathbb{K} := \operatorname{Quot}(A(k,n)) = \operatorname{Quot}(\mathcal{G})(\mathbf{X})$ is a finite separable Galois extension of $\operatorname{Quot}(\mathcal{G})$ with Galois group H. It also follows that for every fixed $i = 1,\ldots,k$, H permutes the variables X_{ij}, which are the roots of $f_i \in \operatorname{Quot}(\mathcal{G})[T]$. Now form the polynomial

$$F := T^n G(\mathbf{X}_1,\ldots,\mathbf{X}_n; -Y_1/T,\ldots,-Y_k/T) = \prod_{j=1}^{n}\left(T - \sum_{i=1}^{k} X_{i,j}Y_i\right).$$

Let $h \in H$. Since h fixes the coefficients of G, it also fixes the coefficients of F, so $h(F) = F$ (where H acts trivially on T and the Y_i). Since the zeros of F, considered as a polynomial in T, are all distinct, there exists $\sigma \in \Sigma_n$ such that

$$\sum_{i=1}^{k} h(X_{i,j})Y_i = \sum_{i=1}^{k} X_{i,\sigma(j)}Y_i$$

for all $j = 1,\ldots,n$. This implies $h(X_{i,j}) = X_{i,\sigma(j)}$ for all i, j. It follows that $H = \Sigma_n$ with 'diagonal action' and $\mathbb{K}^{\Sigma_n} = \operatorname{Quot}(\mathcal{G})$. □

In Hermann Weyl's book 'Classical groups' [16] one can find a proof of the following

Theorem 5.2 *(Weyl). If $\mathbb{Q} \subseteq R$, then $A(k,n)^{\Sigma_n}$ is generated by the coefficients of the Galois-resolvent $G(\mathbf{X}_1,\ldots,\mathbf{X}_n;\mathbf{Y})$. They all have total degree $\leqslant n$, so $\beta(A(k,n)^{\Sigma_n}) \leqslant n$.*

The analogue of Weyl's theorem is false if $R = \mathbb{Z}$ or a field of characteristic $p \leqslant n$. This can be seen from the Σ_2-invariant $\mathfrak{X} := (X_1\cdots X_k)^+ := X_1\cdots X_k + Y_1\cdots Y_k$, which is indecomposable over $\mathbb{Z}$ or $\mathbb{F}_2$ for all $k \in \mathbb{N}$. In [14] it was proved by D. Richman, that the analogue of Weyl's theorem holds if $n!$ is invertible in R (for a different proof using 4.5, see [8]). For arbitrary coefficients the following has been shown in [6].

Theorem 5.3. $\beta(A(k,n)^{\Sigma_n}) \leqslant \max\{n, k\cdot(n-1)\}$ *with equality if $n = p^s$ for a prime p and* char $R = p$, *or* $R = \mathbb{Z}$.

To make use of these results in the context of arbitrary invariant rings, consider a subgroup $H \leqslant G$ with index n and with set of left-cosets

$$G/H := \{H := g_1 H,\ g_2 H,\ \ldots,\ g_n H\}.$$

The left multiplication action of G on the set G/H gives rise to the *Cayley-homomorphism*

$$\rho : G \to \Sigma_{G/H} \cong \Sigma_n, \quad g \mapsto (g_i H \mapsto g_j H := g g_i H).$$

Suppose that $A := R[a_1, \ldots, a_d]$ and $A^H = R[b_1, \ldots, b_k]$ with $b_i \in \mathcal{M}_\beta(\mathbf{a})$ and $\beta := \beta(A^H, \mathbf{a})$. Note that G acts on $A(k,n)$ via ρ; then the map $X_{si} \mapsto g_i(b_s)$ defines a G-equivariant homomorphism $\nu : A(k,n) \to A$ of R-algebras. In fact, ν does not depend on the choice of the g_i and

$$\nu\big(g(X_{si})\big) = \nu(X_{sj}) = g_j(b_s) = g g_i h(b_s) = g g_i(b_s) = g\nu(X_{si}),$$

because $g g_i = g_j h^{-1}$ for a suitable $h \in H$ and $j := \rho(g)(i)$. The map ν for $H = 1$ was used in Emmy Noether's 1916—paper to prove her degree bound in characteristic zero. It is therefore called the *Noether homomorphism*. Since ν is G-equivariant, with the $\rho(G)$-operation on $A(k,n)$, we have

$$\mathcal{N} := \nu\big(A(k,n)^{\Sigma_n}\big) \subseteq A^G.$$

A sharpening of the arguments in 4.1 shows that A^G is purely inseparable over $\mathcal{N}$ and both algebras have the same quotient field. Set $\tilde{G} := \Sigma_n$, $B := A(k,n)$, ν the Noether homomorphism and $\tilde{H} := (\Sigma_n)_1 \cong \Sigma_{n-1}$ be the stabilizer of 1. Then $\rho(H) \leqslant \tilde{H}$, so $\nu(A(k,n)^{\tilde{H}}) \leqslant A^H$. Moreover $\nu(X_{s1}) = g_1(b_s) = b_s$ with $X_{s1} \in A(k,n)^Y$, hence $\nu(A(k,n)^{\tilde{H}}) = A^H$ and we can apply 4.1:

Theorem 5.4. *Let $\tilde{H} := (\Sigma_n)_1 \cong \Sigma_{n-1}$ be the stabilizer of* 1. *Then*

(1) $t_H^G(A^H) = \nu(t_{\tilde{H}}^{\Sigma_n}(A(k,n)^{\tilde{H}})) \subseteq \mathcal{N} \subseteq \nu(A(k,n)^{G/\ker\rho}) \subseteq A^G$.
(2) *For every $0 \neq a \in t_H^G(A^H)$ we have $\mathcal{N}_c = (A^G)_c$. In particular, if A is a domain, then* $\operatorname{Quot}(A^G) = \operatorname{Quot}(\mathcal{N})$.
(3) *Assume that $\mathbb{F}_p \subseteq R$ and let p^r be the maximal p-power dividing n. Then $\sqrt[p^r]{\mathcal{N}} = A^G$.*

Proof. Only (3) does not immediately follow from 4.1: Let $n = p^r q$ with $\gcd(p,q) = 1$. Then

$$\mathfrak{n} := \binom{n}{p^r} \equiv q \not\equiv 0 \mod (p),$$

as can be seen by comparing coefficients of x^{p^r} in the modular identity

$$\sum_{j=0}^{n}\binom{n}{j}x^j = (x+1)^n \equiv \left(x^{p^r}+1\right)^q = \sum_{i=0}^{q}\binom{q}{i}x^{ip^r} \mod (p).$$

Let $h = h(b_1,\dots,b_k) \in A^G$; then we define

$$\Psi := \frac{1}{\mathfrak{n}}\left(\sum \prod_{\ell=1}^{p^r} h(X_{1i_\ell}, X_{2i_\ell},\dots,X_{ki_\ell})\right)$$

where the sum is over all the integer sequences $1 \leqslant i_1 < i_2 < \cdots < i_{p^r} \leqslant n$. It follows that $\Psi \in A(k,n)^{\Sigma_n}$; moreover

$$\nu\big(h(X_{1i_j}, X_{2i_j},\dots,X_{ki_j})\big) = g_{i_j}\big(h(b_1,b_2,\dots,b_k)\big) = h(b_1,b_2,\dots,b_k),$$

hence $\nu(\Psi) = h^{p^r} \in \mathcal{N}$. □

Let $\beta(k,n) := \beta(A(k,n)^{\Sigma_n})$ and $A(k,n)^{\Sigma_n} = R[F_1,\dots,F_s]$ with $F_i \in \mathcal{M}_{\beta(k,n)}(\mathbf{X})$, then $A^G = R[\nu(F_1),\dots,\nu(F_s)]$ with $\nu(F_i) \in \mathcal{M}_{\beta(k,n)\beta}(\mathbf{a}) \cap A^G$. In particular if the index $n = [G:H]$ is invertible in R, then

$$\beta\big(A^G,\mathbf{a}\big) \leqslant \beta(k,n)\beta\big(A^H,\mathbf{a}\big).$$

If p is a prime and R is of characteristic p, then we can take $H = P$, a Sylow p-group of G. Since the index $[G:P]$ is invertible, one can apply 5.4 and construct A^G from A^P via vector invariants. Using 4.7, 5.4 and 5.3 (for $H = 1$) we can summarize:

Theorem 5.5. *Let p a prime with $\mathbb{F}_p \leqslant R$ and let p^r be the maximal p-power dividing $n := |G|$. Assume $A := R[a_1,\dots,a_k]$ is a domain on which G acts by R-algebra automorphisms stabilizing the R-module $\langle a_1,\dots,a_k\rangle$. Let*

$$A(k,n) = R[X_{jg} \mid j = 1,\dots,k,\ g \in G]$$

with Noether-homomorphism

$$\nu : A(k,n) \to A, \quad X_{jg} = g(a_j), \quad \text{and} \quad \mathcal{N} := \nu\big(A(k,n)^{\Sigma_n}\big).$$

Then the following hold:

(1) *There is a $\gamma = (\gamma_1,\dots,\gamma_k) \in \mathbb{N}_0^k$ with $|\gamma| < |G|$ such that $f := t_1^G(\mathbf{a}^\gamma) \neq 0$. For each such f we have $\beta(A_f^G) \leqslant 2|G| - 1$.*

(2) *$t_1^G(A) \subseteq \mathcal{C}(\mathcal{N}, A^G)$ and $A^G = \sqrt[p^r]{\mathcal{N}}$. Furthermore,*

$$\beta(\mathcal{N}) \leqslant \max\big\{|G|, k\big(|G|-1\big)\big\}.$$

(3) *Setting* $B := \mathcal{N}$ *and* $0 \neq c := f$ *we can apply the methods described in* 3.6 *to calculate generators for* $A^G = \mathcal{N} \cap cA$.

6. Explicit localizations and reciprocal rings of invariants

In this section we describe a different but very explicit localization of invariant rings of p-groups over the prime field $\mathbb{F}_p$, which satisfies the conjectured degree bound given in Eq. (2). Of course we have already obtained a better bound for localizations in 4.8, but the localization we are going to describe is of special interest, because it is shared by a new type of "reciprocal ring of invariants," which itself is generated in "negative degree" bounded by $\dim(V)$, independently from $|G|$. The dependence on $|G|$ of the degree bound for the localization arises from the process of "clearing denominators," which involves only explicitly described "norms" of degree $\leqslant |G|$.

Let p be a prime, V a finite-dimensional vector-space over $\mathbb{F}_p$ and $G \leqslant \mathrm{GL}(V)$ a non-trivial p-group. Let V^G denote the subspace of G-fixed points in V and set $n := \dim(V)$ and $m := \dim(V^G)$ so that $1 \leqslant m \leqslant n-1$. Let $S(V) := \mathrm{Sym}(V)$ denote the symmetric algebra of V over $\mathbb{F}_p$ and $S(V)^G$ the ring of G-invariants.

Let $A(V)$ be the $\mathbb{F}_p$-subalgebra of $\mathrm{Quot}(S(V))$ generated by the set $\{v^{-1} \mid v \in V \setminus \{0\}\}$. Then G acts naturally on $A(V)$. Suppose further, as we may, that G stabilizes the flag $\{V_i\}$ in V associated to the basis $\{v_1, v_2, \ldots, v_n\}$ for V with $V^G = V_m$ (here $V_i := \langle v_1, \ldots, v_i \rangle$ for $i = 1, 2, \ldots, n$ and $V_0 := \{0\}$). In [17, Corollary 10.6] it has been shown that the $\mathbb{F}_p$-algebra of G-invariants $A(V)^G$ is generated by the set $\mathcal{T}$ consisting of the v^{-1} for $v \in V^G \setminus \{0\}$ and the orbit sums of products of the form $(u_{m+1}u_{m+2}\cdots u_n)^{-1}$, where each $u_j \in V_j \setminus V_{j-1}$ or $u_j = 1$ (these have "degree" at most $n-m$). This remarkably low degree bound of $n-m$ for $A(V)^G$, which is in stark contrast to the actual and conjectured degree bounds for $S(V)^G$, is accounted for by the miracle of "partial fraction decompositions" and the simple identity

$$(uv)^{-1} = (v-u)^{-1}\big(u^{-1} - v^{-1}\big),$$

which, together with the "degree 1" hsop consisting of the sums $\sum_{u \in V_k} (v_{k+1} + u)^{-1}$ for $k = 0, 1, \ldots, n-1$, enables us to dissipate any build up of "high degree" expressions (as often occurs in $S(V)^G$). (See [17] for a deeper study and further background on $A(V)$ and $A(V)^G$.)

Put $\lambda := \prod_{v \in V \setminus \{0\}} v \in S(V)^G$. Clearly λ is the product of certain *norms* $N(v) := \prod_{w \in v^G} w$, i.e. orbit-products of $v \in V \setminus \{0\}$ under G, each of which is of degree at most $|G|$. Then, as we will see below, one obtains a generating set for the localization $S(V)^G_\lambda$ as an $\mathbb{F}_p$-algebra, which implies

$$\beta'\big(S(V)^G_\lambda\big) \leqslant \max\big\{|G|, (n-m)\big(|G|-1\big)\big\}.$$

Here we have refined the definition of β to β' in order to allow for the inversion of several invariants of degree at most $|G|$. Thus, using the notation of Section 2, if given $c = c_1 c_2 \cdots c_l$ (say), we put

$$\beta'(C_c) := \beta^*(C, c, \mathbf{a})$$
$$:= \min\bigl\{k \in \mathbb{N}_0 \mid c_1, c_2, \ldots, c_l \in \mathcal{M}_k(\mathbf{a}),\ C_c = R\bigl[C \cap \mathcal{M}_k(\mathbf{a}), 1/c\bigr]\bigr\}.$$

Theorem 6.1. *We retain the notation of Section* 6. *In particular $G \leqslant \mathrm{GL}(V)$ is a nontrivial p-group. The localization $S(V)^G_\lambda$ is generated as an $\mathbb{F}_p$-algebra by λ^{-1} (or alternatively by the $N(v)^{-1}$, $v \in V \setminus \{0\}$) and the set $\mathcal{S}$ consisting of the norms $N(v)$, $v \in V \setminus \{0\}$ together with certain orbit-sums of products of vectors of degree at most $(n-m)(|G|-1)$.*

Proof. Clearly the localization $S(V)^G_\lambda$ identifies first with $R = \mathbb{F}_p[v, v^{-1} \mid v \in V \setminus \{0\}]^G$ and hence with the localization $A(V)^G_{\lambda^{-1}}$. Note that there is no ambiguity in notation here since λ is G-invariant. The theorem now follows directly on observing that since the ring R above contain all the norms $N(v)$ and their inverses $N(v)^{-1}$ for nonzero $v \in V$, we may "clear denominators" in the generating set $\mathcal{T}$ above by multiplying each orbit sum with at most $(n-m)$ such norms and thereby obtain the orbit sums in $S(V)^G$ described in $\mathcal{S}$ above. □

Remark 6.2. (1) The invariant ring $A(V)^G$, besides sharing a common localization with $S(V)^G$, is also F-isomorphic to $S(V^*)^G$, i.e. in this case, isomorphic up to pure inseparability (see [17, Lemma 7.2]). In particular this shows that, although the rings $S(V)^G$ and $S(V^*)^G$ can behave quite differently, their fields of fractions are always F-isomorphic (indeed the localization $S(V)^G_\lambda$ and the corresponding $S(V^*)^G_{\lambda^*}$ are F-isomorphic).

(2) We denote by $\mathcal{A}$ the $\mathbb{F}_p$-subalgebra of $S(V)^G$ generated by the norms and orbit sums given in $\mathcal{S}$ above with degrees bounded by

$$\max\bigl\{|G|, (n-m)\bigl(|G|-1\bigr)\bigr\}.$$

Then, at least in principle, we can "grow" $\mathcal{A}$ up to $S(V)^G$ by looking for $f \in \mathcal{A}$ divisible by some norm $N(v)$ in $S(V)^G$ but *not* in $\mathcal{A}$ and then adjoining $fN(v)^{-1} \in S(V)^G$ to $\mathcal{A}$.

Since $S(V)^G$ is integral over $\mathcal{A}$, repeating this procedure a finite number of times will eventually reach $S(V)^G$.

References

[1] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Grad. Stud. Math., vol. 3, Amer. Math. Soc., Providence, RI, 1994.
[2] D.J. Benson, Representations and Cohomology I, Cambridge Stud. Adv. Math., vol. 30, Cambridge Univ. Press, Cambridge, 1995.
[3] W. Bruns, J. Herzog, Cohen–Macaulay Rings, Cambridge Univ. Press, Cambridge, 1993.
[4] H. Derksen, G. Kemper, Computational Invariant Theory, Encyclopaedia Math. Sci., Springer-Verlag, Berlin, 2001, 241 p.
[5] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York, 1995.
[6] P. Fleischmann, A new degree bound for vector invariants of symmetric groups, Trans. Amer. Math. Soc. 350 (4) (1998) 1703–1712.
[7] P. Fleischmann, The Noether bound in invariant theory of finite groups, Adv. Math. 156 (2000) 23–32.

[8] P. Fleischmann, On invariant theory of finite groups, in: H.E.A. Campbell, D.L. Wehlau (Eds.), Invariant Theory in All Characteristics, in: CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 43–69.
[9] P. Fleischmann, G. Kemper, J. Shank, Depth of cohomology modules, Q. J. Math. 55 (2004) 167–184.
[10] J. Fogarty, On Noether's bound for polynomial invariants of a finite group, Electron. Res. Announc. Amer. Math. Soc. 7 (2001) 5–7.
[11] M. Göbel, Computing bases for rings of permutation-invariant polynomials, J. Symbolic Comput. 19 (1995) 285–291.
[12] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann. 77 (1916) 89–92.
[13] E. Noether, Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p, Nachr. Ges. Wiss. Goettingen (1926) 28–35.
[14] D. Richman, Explicit generators of the invariants of finite groups, Adv. Math. 124 (1996) 49–76.
[15] D. Richman, Invariants of finite groups over fields of characteristic p, Adv. Math. 124 (1996) 25–48.
[16] H. Weyl, The Classical Groups, Princeton Univ. Press, Princeton, 1953.
[17] C.F. Woodcock, Reciprocal polynomials and modular invariant theory, 2006, Transform. Groups, in press.